AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) An information recording device for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording device comprising:

a cryptosystem unit that selectively uses a different encryption ~~keys~~ key for each sector ~~sectors~~ from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors;

wherein the data includes ~~the memory stores data including~~ a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

2. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, from among M different encryption keys corresponding to M sectors, which are stored in header information corresponding to the data to be stored in said memory, one encryption key is selected in accordance with a sector in which the

data is stored, and the selected encryption key is used to perform the encryption of data to be stored in each of the sectors.

3. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, from among M different encryption keys corresponding to M sectors, which are stored in header information corresponding to the data to be stored in said memory, a set of at least two encryption keys is selected in accordance with a sector in which the data is stored, and the selected encryption keys are used to perform the encryption of data to be stored in each of the sectors.

4. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, from among P different encryption keys in which the number P differs from the number M, at least one encryption key is selected in accordance with a sector in which the data is stored, and the selected at least one encryption key is used to perform the encryption of data to be stored in each of the sectors.

5. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as single-DES encryption processing using different encryption keys for the sectors.

6. (Original) An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector

is executed as triple-DES encryption processing using at lest two different encryption keys for each of the sectors.

7. (Original) An information recording device according to claim 1, wherein said cryptosystem unit selectively executes one of sector-independent encryption processing in which in accordance with an encryption format type stored in header information corresponding to the data to be stored in said memory, the entirety of the data is encrypted in a single encryption mode, and sector-dependent encryption processing in which in accordance with the encryption format type, the data is encrypted by using encryption keys which are selected for the sectors.

8. (Currently Amended) An information playback device for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number said information playback device comprising:

a cryptosystem unit which selectively uses a different decryption ~~keys~~ key for each sector ~~sectors~~ from the first sector to the M-th sector to execute decryption processing and the cryptosystem unit executes decryption processing on data stored in each of the sectors;

wherein the data includes ~~the memory stores data including~~ a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a

block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

9. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, from among M different decryption keys corresponding to M sectors, which are stored in header information corresponding to data stored in said memory, one decryption key is selected in accordance with a sector in which the data is stored, and the selected decryption key is used to perform the decryption of data stored in each of the sectors.

10. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, from among M different decryption keys corresponding to M sectors, which are stored in header information corresponding to data stored in said memory, a set of at least two decryption keys is selected in accordance with a sector in which data is stored, and the selected encryption keys are used to perform the decryption of data stored in each of the sectors.

11. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, from among P different decryption keys in which the number P differs from the number M, at least one decryption key is selected in accordance with

a sector in which data is stored, and the selected at least one decryption key is used to perform the decryption of data stored in each of the sectors.

12. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as single-DES decryption processing using different decryption keys for the sectors.

13. (Original) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as triple-DES decryption processing using at lest two different decryption keys for each of the sectors.

14. (Original) An information playback device according to claim 8, wherein said cryptosystem unit selectively executes one of sector-independent decryption processing in which in accordance with an encryption format type stored in header information corresponding to data stored in said memory, the entirety of the data is decrypted in a single decryption mode, and sector-dependent decryption processing in which in accordance with the encryption format type, the data is decrypted by using decryption keys which are selected for the sectors.

15. (Currently Amended) An information recording medium having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors

from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number,

wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area,

wherein the storage area stores data including a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a block permission table for accessing a permission table that describes memory access control information, and

wherein an integrity check of the integrity of the revocation list and block permission table is performed.

16. (Original) An information recording medium according to claim 15, wherein said plurality of different cryptographic keys are M different encryption keys corresponding to the M sectors.

17. (Currently Amended) An information recording method for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording method comprising: ~~a data encrypting step~~

~~in which~~ encryption processing ~~on~~ data to be stored in the sectors ~~is executed~~ by performing encryption using a different encryption ~~keys selected~~ key for each sector from the first sector to the M-th sector;

storing ~~the memory stores~~ data including a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a block permission table for accessing a permission table that describes memory access control information; and

performing ~~wherein~~ an integrity check of the revocation list and the block permission table ~~is performed~~.

18. (Currently Amended) An information recording method according to claim 17, further comprising ~~wherein said data encrypting step comprises the steps of~~:

selecting, from among M different encryption keys corresponding to the M sectors, the M different encryption keys being stored in header information corresponding to the data to be stored in said memory, one encryption key in accordance with a sector in which the data is stored; and

performing the encryption based on the selected encryption key of data to be stored in each of the sectors.

19. (Currently Amended) An information recording method according to claim 17, further comprising ~~wherein said data encrypting step comprises the steps of~~:

selecting, from among M different encryption keys corresponding to the M sectors, the M different encryption keys being stored in header information corresponding to the data to be stored in said memory, a set of at least two encryption keys in accordance with a sector in which the data is stored; and

performing the encryption based on the selected encryption keys of data to be stored in each of the sectors.

20. (Currently Amended) An information recording method according to claim 17, further comprising ~~wherein said data-encrypting step comprises the steps of~~:

selecting, from among P different encryption keys stored in header information corresponding to the data to be stored in said memory, in which the number P differs from the number M, at least one encryption key in accordance with a sector in which the data is stored; and

performing the encryption based on the at least one encryption key of data to be stored in each of the sectors.

21. (Currently Amended) An information recording method according to claim 17, wherein~~, in said data-encrypting step,~~ the encryption processing is executed as single-DES encryption processing using different encryption keys for the sectors.

22. (Currently Amended) An information recording method according to claim 17, wherein~~, in said data-encrypting step,~~ the encryption processing is executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors.

23. (Currently Amended) An information recording method according to claim 17, further comprising: ~~a determination step for~~

determining which type of processing should be executed between sector-independent encryption processing in which in accordance with an encryption format type stored in header information corresponding to the data to be stored in said memory, the entirety of the data is encrypted in a single encryption mode, and sector-dependent encryption processing in which in accordance with the encryption format type, the data is encrypted by using encryption keys which are selected for the sectors, wherein one of said sector-independent encryption processing and said sector-dependent encryption processing is selectively executed based on the determination in said determination step.

24. (Currently Amended) An information playback method for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information playback method comprising: ~~a data decrypting step~~

decrypting ~~in which decryption of~~ data stored in each of the sectors ~~is performed~~ by executing decryption processing using a different decryption ~~keys selected in accordance with~~ key for each sector from the first sector to the M-th sector;

storing ~~the memory stores~~ data including a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a block permission table for accessing a permission table that describes memory access control information; and

performing an integrity check ~~checking unit checks the integrity of~~ the revocation list and the block permission table.

25. (Currently Amended) An information playback method according to claim 24, further comprising ~~wherein said data decrypting step comprises the steps of~~:

selecting, from among M different decryption keys corresponding to the M sectors, which are stored in header information corresponding to data stored in said memory, one decryption key in accordance with a sector in which data is stored; and

performing the decryption based on the selected decryption key of data stored in each of the sectors.

26. (Currently Amended) An information playback method according to claim 24, further comprising ~~wherein said data decrypting step comprises the steps of~~:

selecting, from among M different decryption keys corresponding to the M sectors, the M different decryption keys being stored in header information corresponding to data stored in said memory, a set of at least two decryption keys in accordance with a sector in which data is stored; and

performing the decryption based on the selected decryption keys of data stored in each of the sectors.

27. (Currently Amended) An information playback method according to claim 24, further comprising ~~wherein said data decrypting step comprises the steps of~~:

selecting, among from P different decryption keys stored in header information corresponding to data stored in said memory, in which the number P differs from the number M, at least one decryption key in accordance with a sector in which data is stored; and

performing the decryption based on the selected decryption keys of data stored in each of the sectors.

28. (Currently Amended) An information playback method according to claim 24, wherein the decryption processing ~~said data decrypting step~~ is executed as single-DES decryption processing using different decryption keys for the sectors.

29. (Currently Amended) An information playback method according to claim 24, wherein the decryption processing ~~said data decrypting step~~ is executed as triple-DES decryption processing using at least two decryption keys for each of the sectors.

30. (Currently Amended) An information playback method according to claim 24, further comprising: ~~a determination step for~~

determining which type of decryption processing should be executed between sector-independent decryption processing in which in accordance with an encryption format type stored in header information corresponding to data stored in said memory, the entirety of the data is decrypted in a single decryption mode, and sector-dependent decryption processing in which in accordance with the encryption format type, the data is decrypted by using decryption keys which are selected for the sectors, wherein one of

said sector-independent decryption processing and said sector-dependent decryption processing is selectively executed based on the determination in said determination step.

31. (Currently Amended) A computer-readable ~~program-providing~~ medium comprising ~~for providing~~ a computer program product for performing, when executed by a processor, a data encryption method comprising: ~~which controls a computer system to execute processing which~~

storing ~~stores~~ data in a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number;~~, said computer program product comprising a data encrypting step~~

~~in which~~ encryption processing ~~on~~ data to be stored in the sectors ~~is executed~~ by performing encryption using a different encryption ~~keys selected for~~ key for each sector from the first sector to the M-th sector;

storing ~~the memory stores~~ data including a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a block permission table for accessing a permission table that describes memory access control information; and

checking ~~an integrity checking unit checks~~ the integrity of the revocation list and the block permission table.

32. (Currently Amended) A computer readable ~~program providing~~ medium comprising ~~for providing~~ a computer program product for performing, when executed by a processor, a data decryption method comprising: ~~which controls a computer system to execute processing which~~

reading ~~reads~~ data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number;~~, said computer program product comprising~~

~~a data decrypting step in which~~

decrypting ~~decryption of~~ data stored in each of the sectors ~~is performed~~ by executing decryption processing using a different decryption ~~keys selected in accordance with~~ key for each sector from the first sector to the M-th sector;

storing ~~the memory stores~~ data including a revocation list having revocation information regarding revoked media or content ~~on each media~~ and a block permission table for accessing a permission table that describes memory access control information; and

checking ~~an integrity checking unit checks~~ the integrity of the revocation list and the block permission table.